State of Iowa Enterprise Best Practices for use of Social Networking Sites
October 30, 2009

Purpose

Due to the prevalence and rapid growth of social networking on the internet, the Information Security Office has reviewed these technologies, evaluated the risks, and identified current application usage within government. Agencies should review all aspects of social networking and decide how it will be used in their agency. This summary is designed to assist agencies in the decision making process of whether or not to utilize these technologies and if so, how to do so in a secure manner.

Definition

Social Networking Sites are websites or services where people can contribute content and share information with others. This information typically includes photos, videos, text, news, blogs, profiles and current event information. This content is easily uploaded to the internet and modified as needed. As with all internet postings, once it posted it cannot be permanently removed. Popular social networking sites include but are not limited to: YouTube, Flickr, MySpace, Twitter and Facebook.

Use in Government

Federal, state and local government have adopted these technologies as a means to actively and quickly communicate with their citizens and each other in order to promote open government. Several states, including the State of Iowa, provide links to social networking sites to broadcast information about current events, promote opportunities and to quickly disseminate information with their constituents.

Guidelines and Recommendations

The popularity of these sites has also attracted computer hackers and organized crime. Social networking sites are currently the most prevalent target for cyber attacks. If agencies adopt these technologies, they need to be aware of the associated risks and address these risks through policy, technology and training.

1. **Policy:** Establish a policy describing the acceptable/unacceptable use of social networking sites within the agency. Include the following topics:
    - Creation and maintenance of agency sponsored sites,
    - Agency postings to non-agency sponsored sites,
    - Use of agency computers to access social networking sites, and
    - Use of personal devices to access social networking sites during work hours.
    - Review period for the policy. The policy should be reviewed annually.

2. **Terms of Service:** Use of these sites is subject to the terms of service agreement of the provider. These terms may not be amenable to your agency and should be reviewed by your legal staff. Specific topics may include:
    - Perceived endorsement of the website by your agency,
    - Perceived affiliation with advertisers placed with your agency content, and
    - Availability, modification and redistribution of your content.

3. **Personal Devices**: Social networking sites and internet access are readily available from personal cell phones, iPhones, netbooks and other devices.
    - State owned technology cannot today monitor, filter or restrict access to these personal devices, and
    - iPods, MP3 players and similar devices are not allowed to be connected to state owned property including computers or networks.
    - Personal computers and cell phones are not allowed to be connected to state owned property including computers or networks without management approval.
    - Personal computers and cell phones used for state business must meet the requirements of the enterprise security standards.

4. **Agency Sponsored Sites**: Agency sponsored use of social networking sites:
    - Should require management approval,
    - Shall include a statement which defines the purpose and scope associated with use of the site,
    - Shall not include confidential agency information,
    - Are subject to Open Records requirements, and
    - Must include a statement that any content posted is subject to public disclosure.

5. **Postings**: Official agency postings to non-agency sponsored social networking sites:
    - Should require management approval,
    - Should be clearly identified with employee and agency name,
    - Shall not include confidential agency information, and
    - Shall not violate copyright law.

6. **Site Blocking:** Agencies may choose to limit or block access to these sites.
    - Web Filtering software can block, filter, report and track usage of these sites, and
    - Firewall settings can block specific sites and exceptions can be made to allow individuals access as needed.

7. **Awareness Training:** Employees with access to these sites need to recognize the security risks. Some of the recommended information security guidelines agencies should follow include:

    - **Usage and prevention**
        - Use of state computer equipment is for official state business only.
        - For devices accessing these sites, ensure anti-virus is current.
        - Ensure anti-spyware is current.
        - Ensure that operating system and application patches are applied.
        - Ensure that application updates and patches are applied.

    - **URL Shortening**
        - URL shortening tools, such as tinyurl and Bit.ly, conceal the actual website link and can direct users to malicious websites.

- URL shortening is typically used in twitter because of the 140 character limit.

- **Social Engineering/Phishing**
  - These sites are the #1 target for social engineering, phishing and malware attacks.
  - Identities are anonymous on the web; you may not be communicating with whom you think you are.

- **Passwords**
  - Never use your State of Iowa username or password or credentials on these sites.
  - Strong and unique passwords must be used for each individual website.

- **Privacy**
  - Confidential information should never be posted to any social networking sites.
  - Professional and personal content on these sites should never be mixed.
  - Don't share personal information, travel plans or information about others without their consent.
  - Enable and utilize privacy features included with the social networking sites.

- **Malware**
  - Custom written video players may contain malware; think twice before you click.
  - Do not visit unknown or un-trusted websites.
  - Websites can redirect and download malware to your computer if not patched.
  - Do not download files from linked websites you do not know or trust.
  - Malicious files can be in the form of commonly accepted file formats such as PDF documents, Microsoft Office products and others.

- **Reporting**
  - Work with your IT staff to ensure your computer is properly patched.
  - Always report incidents promptly to your Information Security Officer or the State the Information Security Office.

Additional Information

For more information on social networking sites, please contact the Information Security Office at 515-281-4820. The Information Security Office can assist agencies with technology solutions, equipment configurations, training and awareness and internal policy development.

Source: DAS-Information Security Office